



啟用多因素驗證 Element Software

NetApp
October 01, 2024

目錄

啟用多因素驗證	1
設定多因素驗證	1
多因素驗證的其他資訊	1

啟用多因素驗證

多因素驗證 (MFA) 透過安全聲明標記語言 (SAML) 使用第三方身分識別供應商 (IDP) 來管理使用者工作階段。MFA可讓系統管理員視需要設定其他驗證因素、例如密碼和文字訊息、密碼和電子郵件訊息。

設定多因素驗證

您可以透過Element API使用這些基本步驟、將叢集設定為使用多因素驗證。

有關每種 API 方法的詳細信息"[Element API參考](#)"，請參閱。

1. 透過呼叫下列 API 方法並以 JSON 格式傳遞 IDP 中繼資料、為叢集建立新的第三方身分識別提供者 (IDP) 組態：CreateIdpConfiguration

IDP中繼資料以純文字格式從第三方IDP擷取。此中繼資料必須經過驗證、以確保其在Json中正確格式化。您可以使用許多 JSON 格式化板應用程式、例如：<https://freeformatter.com/json-escape.html>。

2. 透過 spMetadataUrl 擷取叢集中繼資料、以呼叫下列 API 方法複製到協力廠商 IDP：
ListIdpConfigurations

SpMetadataUrl是一個URL、用於從叢集擷取IDP的服務供應商中繼資料、以建立信任關係。

3. 在協力廠商IDP上設定SAML斷言、以納入「NameID」屬性、以唯一識別使用者進行稽核記錄、並讓「單一登出」正常運作。
4. 透過呼叫下列 API 方法、建立一個或多個由第三方 IDP 驗證的叢集管理員使用者帳戶、以進行授權：
AddIdpClusterAdmin



IDP叢集管理員的使用者名稱應與SAML屬性名稱/值對應相符、以取得所需的效果、如下列範例所示：

- email=bob@company.com -其中IDP已設定為在SAML屬性中釋出電子郵件地址。
- Group=cluster系統管理員：其中IDP設定為釋放所有使用者應有存取權的群組內容。請注意、為了安全起見、SAML屬性名稱/值配對區分大小寫。

5. 透過呼叫下列 API 方法、為叢集啟用 MFA：EnableIdpAuthentication

如需詳細資訊、請參閱

- "[零件與元件軟體文件SolidFire](#)"
- "[vCenter Server的VMware vCenter外掛程式NetApp Element](#)"

多因素驗證的其他資訊

您應該瞭解下列有關多因素驗證的注意事項。

- 為了重新整理不再有效的 IDP 憑證、您需要使用非 IDP 管理員使用者來呼叫下列 API 方法：

UpdateIdpConfiguration

- MFA與長度小於2048位元的憑證不相容。根據預設、會在叢集上建立一個2048位元SSL憑證。在呼叫 API 方法時、您應該避免設定較小的憑證： `SetSSLCertificate`



如果叢集使用的憑證在升級前低於2048位元、則叢集憑證必須在升級至Element 12或更新版本之後、以2048位元或更高的憑證進行更新。

- IDP管理使用者無法直接（例如透過SDK或Postman）撥打API呼叫、也無法用於其他整合（例如OpenStack Cinder或vCenter外掛程式）。如果您需要建立具有這些功能的使用者、請新增LDAP叢集管理使用者或本機叢集管理使用者。

如需詳細資訊、請參閱

- ["使用Element API管理儲存設備"](#)
- ["零件與元件軟體文件SolidFire"](#)
- ["vCenter Server的VMware vCenter外掛程式NetApp Element"](#)

版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。